De dynamiek van cybercrimewetgeving in Europa en Nederland

Koops, E.J.

Published in:
Justitiële verkenningen: Documentatieblad van het Ministerie van Justitie

Publication date:
2012

Document Version
Publisher's PDF, also known as Version of record

De dynamiek van cybercrime-wetgeving in Europa en Nederland

B.J. Koops*

Grensoverschrijdende misdaad is niet van vandaag of gisteren. Inmiddels is er dan ook de nodige ervaring met grensoverschrijdende misdaadbestrijding. Toch brengt cybercrime – misdaad met behulp van of gericht tegen computernetwerken – nieuwe uitdagingen met zich mee. Waar 'klassieke' misdaad, zoals drugscriminaliteit of wapen- en mensensmokkel, nog altijd fysiek van aard is met mensen en objecten die de grens overgaan, speelt cybercriminaliteit zich af op moeilijk grijpbare plaatsen (gemakshalve cyberspace genaamd). Daarbij gaan alleen bits en bytes de grens over. Internet als locus delicti kent diverse eigenschappen die cybercrime tot een specifiek probleem maken: het is wereldwijd, gedeterritorialiseerd, flexibel en snel ontwikkelend; het faciliteert een informatie-economie die in toenemende mate rond gegevens (in plaats van goederen) draait; en het faciliteert voor misdadigers nieuwe manieren om op afstand, geautomatiseerd en tegen grote groepen potentiële slachtoffers tegelijk strafbare feiten te plegen (Koops, 2010a). Dit betekent dat cybercrime *inherent* grensoverschrijdend is en minder natuurlijke drempels kent dan klassieke grensoverschrijdende misdaad.

Dit roept de vraag op of het straf(proces)recht, dat van oudsher sterk nationaal georiënteerd is vanwege het grote belang van nationale soevereiniteit, wel is toegesneden op de bestrijding van cybercrime. Kan de wetgever snel genoeg inspelen op technische ontwikkelingen, en is er voldoende internationale afstemming om dit grensoverschrijdende fenomeen aan te pakken? In deze bijdrage belicht ik deze vragen door de dynamiek van cybercrimewetgeving in kaart te brengen. Ik kijk in het bijzonder naar de wisselwerking tussen Europees en Nederlands recht. Na een korte schets van de geschiedenis van de cybercrimewetgeving tot nu toe, bespreek ik

* Prof. dr. Bert-Jaap Koops is hoogleraar regulering van technologie bij TILT – Tilburg Institute for Law, Technology, and Society van de Universiteit van Tilburg.

diverse voorbeelden van de wederzijdse verhouding tussen Europese en nationale initiatieven. Daaruit leid ik vervolgens af hoe de dynamiek van cybercrimewetgeving er op hoofdlijnen uitziet. In de afsluitende beschouwing bespreek ik of deze dynamiek in staat lijkt om de wetgeving voldoende toe te rusten om cybercrime effectief te bestrijden in de wereldwijde, dynamische context van internet. Vanwege de beperkte omvang van deze bijdrage kan ik veelal niet de achtergrond van de gegeven voorbeelden uitdiepen; ik verwijs de geïnteresseerde lezers daarvoor naar eerdere uitgebreidere beschrijvingen (Koops, 2007; 2010b). Ik gebruik verder de termen cybercrime en computercriminaliteit als synoniemen in deze bijdrage.

Een korte geschiedenis van cybercrimewetgeving

Europa

In de jaren tachtig drong het besef door dat computers ook een object of hulpmiddel van misdadigers waren. Sommige landen pasten hun wetgeving aan en internationaal gaf de OESO richtlijnen voor welke computerhandelingen strafbaar zouden moeten worden (OECD, 1986). Ook de Raad van Europa boog zich over computercriminaliteit, met aanbevelingen op materieel (1989) en procedureel (1995) gebied.[1] Toen de aanbevelingen wel erg vrijblijvend bleken, werd besloten een bindend verdrag op te stellen. Dat leidde tot het Cybercrime-Verdrag (hierna: CCV) van de Raad van Europa, dat in 2001 in Boedapest werd ondertekend en in 2004 in werking trad.[2] Omdat de Verenigde Staten bij de voorbereiding betrokken waren en gehoopt werd dat zij partij zouden worden (wat in 2007 ook zou gebeuren), werd de strafbaarstelling van racistische uitlatingen niet in het verdrag opgenomen (die voor de Verenigde Staten onaanvaardbaar zou zijn wegens het Eerste Amendement over vrije meningsuiting), maar in een Aanvullend Protocol van de

1 Council of Europe, Recommendation R(89) 9 on computer-related crime; Recommendation R(95) 13 concerning problems of criminal procedural law connected with information technology.

2 Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Trb. 2002, 18. Zie http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG.

Raad van Europa.[3] Een ander urgent onderwerp met een belangrijke cyberdimensie – het seksueel misbruiken van minderjarigen – werd geregeld in het Verdrag van Lanzarote, dat in 2010 in werking trad.[4] Ondertussen zat het andere Europa, de Europese Unie, niet stil. Aangezien het CCV niet door alle EU-leden was geratificeerd, werd de behoefte gevoeld om voor de EU-lidstaten bindende regels te stellen voor computercriminaliteit. Dit leidde tot drie kaderbesluiten, over fraude met niet-chartaal geld, aanvallen op computersystemen en seksuele uitbuiting van kinderen en kinderpornografie.[5] Daarnaast is er niet-bindend Europees beleid dat beoogt om lidstaten een stap verder te brengen in de strijd tegen computermisdaad en aanpalende gebieden.[6]

De internationale, en met name Europese, benadering van cybercrimewetgeving is aldus een poging om nationale wetgeving dichter bij elkaar te brengen, maar er is – vanwege het grote belang van nationale soevereiniteit op het gebied van strafrecht – op veel punten geen internationale dwingende regelgeving. De EU-kaderbesluiten stellen een minimum aan strafbaarstellingen in de Europese Unie, maar gaan niet in op opsporingsbevoegdheden; het CCV heeft wel een behoorlijk palet aan strafbaarstellingen en opsporingsbevoegdheden, maar met de nodige uitzonderingsclausules, en bovendien is er geen verplichting voor landen om zich bij het verdrag aan te sluiten. Cybercrimewetgeving is vooral een landschap van samenwerking, gebaseerd op harmonisatie van nationale materiële en procedurele wetgeving waar mogelijk, maar vooral ook op juridische en praktische stimulering van rechtshulp (Sieber, 2010, p. 87).

3 Aanvullend Protocol betreffende de strafbaarstelling van handelingen van racistische of xenofobische aard verricht via computersystemen, Trb. 2005, 46. Zie http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CL=ENG.

4 Verdrag inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik, Trb. 2008, 58. Zie http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CL=ENG.

5 Kaderbesluiten 2005/222/JHA, 2004/68/JBZ en 2005/222/JHA. De kaderbesluiten worden momenteel herzien, zie bijvoorbeeld Proposal for a Directive on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, COM(2010)517 final.

6 Europese Commissie, Naar een algemeen beleid voor de bestrijding van cybercriminaliteit, COM(2007)267def.

Nederland

Nederland voerde in 1993 omvangrijke wetgeving in met de Wet computercriminaliteit. Deze wet kwam tot stand op basis van aanbevelingen van de Commissie Computercriminaliteit (1987) en een gedegen discussie daarover in de literatuur (bijvoorbeeld Kaspersen, 1990; Wiemans, 1991) en het parlement.[7] Naast strafbaarstelling van de belangrijkste vormen van computercriminaliteit bevatte de wet ook een uitvoerige regeling van computergerelateerde opsporingsbevoegdheden. Vanwege de ontwikkelingen in de techniek ontstond al snel behoefte aan actualisering van de wetgeving. Het wetsvoorstel Computercriminaliteit II uit 1999 werd echter ingehaald door Europese ontwikkelingen, met name het CCV dat moest worden geïmplementeerd. Pas in 2006 trad de Wet computercriminaliteit II (hierna ook: CCII) in werking,[8] kort na de inwerkingtreding van de goedkeuringswet van het CCV.[9] De wet CCII voerde enkele nieuwe strafbepalingen in, bijvoorbeeld over verstikkingsaanvallen (*denial-of-service attacks*), en paste op onderdelen het materiële en procedurele strafrecht aan. In 2010 werd vervolgens een wetsvoorstel versterking bestrijding computercriminaliteit in consultatie gegeven dat enkele overgebleven onderwerpen zou regelen, zoals een bevel illegale inhoud van internet te verwijderen en heling van gegevens;[10] Hoewel het zwaartepunt van Nederlandse cybercrimewetgeving ligt bij de Wet computercriminaliteit en zijn opvolgers, zijn ook de nodige andere wetten van belang; sommige daarvan regelen een voor computercriminaliteit belangrijk thema, zoals seksueel misbruik van kinderen[11] of het vorderen van gegevens,[12] andere zijn meer algemene wetten met een relevante bepaling, zoals

7 Kamerstukken II 1989/90, 21 551, nr. 1-3; Stb. 1993, 33.
8 Stb. 2006, 300.
9 Stb. 2006, 299.
10 Conceptwetsvoorstel versterking bestrijding computercriminaliteit (hierna: wetsontwerp), www.internetconsultatie.nl/wetsvoorstel_versterking_bestrijding_computercriminaliteit. Ik ben overigens van mening dat het wetsvoorstel nog wel meer zou mogen regelen, en dus beter Computercriminaliteit III kan heten (Koops, 2010c, p.). Het wachten is nog op het indienen van een dergelijk wetsvoorstel bij het parlement.
11 Wet partiële wijziging zedelijkheidswetgeving, Stb. 2002, 388; Wet tot uitvoering van het te Lanzarote totstandgekomen Verdrag (...), Stb. 2009, 544.
12 Wet vorderen gegevens telecommunicatie, Stb. 2004, 105; Wet bevoegdheden vorderen gegevens, Stb. 2005, 390.

de strafbaarstelling van *phishing* (het hengelen naar, vooral financiële, gegevens) in een antiterrorismewet.[13]

De dynamiek van Europese en nationale cybercrimewetgeving, vooral de verhouding tussen Europees en nationaal recht, kent een aantal facetten. De hiernavolgende paragrafen schetsen verschillende vormen van beïnvloeding, toegelicht aan de hand van illustratieve voorbeelden.

Directe invloed van Europa op Nederland

Ten eerste zien we directe Europese invloed op de Nederlandse wetgeving in de invoering of formulering van bepaalde strafbepalingen. Het strafbaar stellen van 'grooming' – het via internet benaderen van minderjarigen en vervolgens een ontmoeting afspreken met het oog op seksueel misbruik – en van het zich opzettelijk toegang verschaffen tot kinderporno (denk aan het betalen voor een webpagina met stromende kinderpornobeelden) zijn rechtstreekse uitwerkingen van het Verdrag van Lanzarote.
Vaak is de Europese invloed zichtbaar in een aangepaste formulering van een reeds door Nederland voorgenomen strafbepaling. Een voorbeeld daarvan is de strafbaarstelling van het verhinderen van iemands toegang tot een computer in artikel 138b Wetboek van Strafrecht (Sr); dit artikel was in wetsvoorstel Computercriminaliteit II beperkt tot 'e-mailbommen', maar ter implementatie van artikel 5 CCV werd dit uitgebreid tot elke vorm van toegangsbelemmering van computers, zodat het nu ook de in de praktijk steeds meer voorkomende verstikkingsaanvallen omvat.[14] Een ander voorbeeld is de regeling van aansprakelijkheid van internetaanbieders. Het wetsvoorstel CCII uit 1999 bevatte een regeling die niet strookte met de kort daarna ingevoerde Richtlijn elektronische handel (2000/31/EG), zodat de Europese Commissie een *standstill*-beschikking uitvaardigde voor het wetsvoorstel.[15] Die stilstandperiode werd vervolgens

13 Wet in verband met de strafbaarstelling van het deelnemen en meewerken aan training voor terrorisme (...) en enkele andere wijzigingen, Stb. 2009, 245; deze wet wijzigde art. 326 Sr (oplichting).
14 Zie art. 138b in Kamerstukken II 1998/99, 26 671, nr. 1-2 en Kamerstukken II 2004/05, 26 671, nr. 7.
15 Kamerstukken II 1999/2000, 26 671, nr. 5.

gebruikt om het wetsvoorstel ingrijpend aan te passen aan het CCV, terwijl de regeling van internetaanbiederaansprakelijkheid (art. 54a Sr) verhuisde naar de implementatiewet e-handel.[16] Waar de Europese regelgeving hier een vertragend effect had op de Nederlandse wetgeving, kan het echter ook een stimulans zijn om een wetsvoorstel door te voeren. Het initiatiefwetsvoorstel tot strafbaarstelling van 'negationisme' (het ontkennen van genocide) lag lange tijd te verstoffen in de Tweede Kamer, totdat het – mogelijk mede onder invloed van het Aanvullend Protocol over internetracisme, dat expliciet om een strafbaarstelling van negationisme vraagt – begin 2010 alsnog nader werd behandeld.[17]

Inhoudelijke invloed van Europa op Nederland

Ten tweede is een Europese invloed op de inhoud van Nederlandse wetgeving zichtbaar die verder gaat dan het (her)formuleren van strafbepalingen om nieuwe technische ontwikkelingen af te dekken. Soms herziet de Nederlandse wetgever eerder gemaakte beleidskeuzes in de wetgeving onder invloed van Europese regelgeving. Een prominent voorbeeld daarvan is de strafbaarstelling van kinderpornografie. Bij de implementatie van het CCV werd niet alleen de leeftijdsgrens opgehoogd van 16 naar 18 jaar, maar werd ook de ratio van strafbaarstelling herzien. Nederland baseerde de wetgeving voorheen op de grondslag om feitelijk seksueel misbruik van kinderen te bestrijden; dat betekende dat plaatjes waarvoor geen kinderen zijn misbruikt – zoals met de computer gegenereerde plaatjes ('virtuele kinderporno') of met een telelens gemaakte foto's van kinderen op een naaktstrand – niet strafbaar waren. Het CCV hanteerde echter als grondslag van strafbaarstelling het bestrijden van een subcultuur van kindermisbruik en stelde daarom ook virtuele kinderporno strafbaar; dergelijke plaatjes kunnen immers gewenning veroorzaken voor pedofielen (waarna ze mogelijk afglijden tot feitelijk misbruik) en ook worden gebruikt om kinderen te verleiden tot het 'toestemmen' in seksuele handelingen. Onder invloed van deze Europese regelgeving wijzigde Nederland de ratio

16 Aanpassingswet richtlijn inzake elektronische handel, Stb. 2004, 210.
17 Kamerstukken II 2010/11, 30 579, nr. 9, p. 6-7.

van strafbaarstelling, zodat ook voorheen 'onschuldige' plaatjes – inclusief naaktstrandfoto's – onder het bereik kwamen.[18]
Een andere systematische wijziging betrof het aftappen van communicatie; traditioneel is dat gericht op het onderscheppen van openbare telecommunicatie (zoals de vroegere PTT), maar onder invloed van het CCV breidde de Nederlandse wetgever de bevoegdheid uit tot alle beroepsmatige communicatieaanbieders, zoals bedrijven met een intern telefoon- en elektronisch netwerk voor werknemers. Dit is een ingrijpende systematische wijziging, omdat veel meer organisaties nu onder het bereik van aftapwetgeving vallen, die echter nauwelijks inhoudelijk bediscussieerd is in het parlement; men nam kennelijk aan dat het ging om een verplichte implementatie van internationale regels die als zodanig niet te bediscussiëren viel. Vermoedelijk vanwege de complexiteit van de Nederlandse wetgeving rond aftappen – in de spaghettikluwen van de 126-serie in het Wetboek van Strafvordering (Sv) – is het aanpassen van de wetgeving daarbij ook niet helemaal doorgevoerd; op enkele plaatsen spreekt de wet nog van 'openbare telecommunicatie' (zie Koops, 2010b, p. 34).
Een andere inhoudelijke wijziging betreft computervredebreuk (*hacken*), dat in 1993 strafbaar werd gesteld, mits daarbij enige beveiliging werd doorbroken of de toegang door slinkse of technische ingrepen werd verschaft. De wetgever nam deze beveiligingseis op als signaal aan gebruikers dat het belangrijk is hun computer te beveiligen – iets wat rond 1990 nog geen gemeengoed was. Onder invloed van het CCV en het Kaderbesluit aanvallen op informatiesystemen heeft de wetgever echter in 2006 de beveiligingseis laten vallen; de Europese regelgeving stond weliswaar toe dat lidstaten een beveiligingseis stellen, maar de overige in artikel 138a (oud) Sr genoemde methoden (technische ingreep, valse signalen of een valse hoedanigheid) pasten daar niet bij. Wat mij betreft had de wetgever hier beter de beveiligingseis kunnen handhaven (omdat de alternatieve methoden feitelijk alleen aan de orde zijn als de computer enige vorm van beveiliging kent), vanwege het belangrijke signaal aan gebruikers over computerbeveiliging. De Europese regels verzetten zich daar niet tegen. Hier zien we dan ook dat de Nederlandse wetgeving niet verandert onder invloed van dwingende

18 Wet partiële wijziging zedelijkheidswetgeving, Stb. 2002, 388; Aanwijzing kinderpornografie, Stcrt. 23 augustus 2007, nr. 162, p. 8.

Europese regels, maar doordat de wetgever een eigen interpretatie kiest van Europese regels.
Iets soortgelijks zien we ook bij misbruik van hulpmiddelen (art. 6 CCV), waarbij tal van voorbereidingshandelingen voor computercriminaliteit – zoals het maken, verspreiden of in bezit hebben van virusprogramma's of wachtwoorden om computers te hacken – strafbaar zijn gesteld, vooral om de groeiende zwarte markt in dergelijke hulpmiddelen te bestrijden. De Nederlandse wetgever heeft ervoor gekozen om de voorbereidingshandeling met dezelfde maximumstraf te bedreigen als het doeldelict (zie art. 139d lid 2 en 161sexies lid 2 Sr). Dit wijkt af van het systeem van de Nederlandse wet, waarin voorbereidingshandelingen een maximumstraf hebben die de helft is van die van het doeldelict (art. 46 Sr). Deze systeemafwijking is niet echt overtuigend beargumenteerd door de wetgever (Koops, 2010b, p. 627) en wordt in elk geval niet afgedwongen door de Europese regelgeving.

Geen invloed van Europa op Nederland

Ten derde zijn er ook veel gevallen waarin de Nederlandse wetgeving helemaal niet is beïnvloed door Europese regelgeving.
Dit zien we vooral wanneer nieuwe vormen van computercriminaliteit ontstaan, veelal door technische ontwikkelingen, die nog niet in Europese instrumenten zijn afgedekt. Zo is er de laatste jaren veel discussie over strafbaarstelling van identiteitsdiefstal (De Vries e.a., 2007; Van der Meulen, 2011). Een belangrijk onderdeel van identiteitsdiefstal is phishing, het 'hengelen' naar financiële en andere persoonsgegevens waarmee vervolgens diensten kunnen worden afgenomen op naam van iemand anders. De Nederlandse wetgever stelde phishing strafbaar door de oplichtingsbepaling (art. 326 Sr) aan te passen zodat ook het aftroggelen van gegevens strafbaar is.[19] Dit was niet geregeld in het CCV, noch in het Kaderbesluit fraude met niet-chartaal geld.
Een ander voorbeeld van zelfstandige nationale ontwikkeling van cybercrimewetgeving is de interpretatie van het begrip 'goed' in het strafrecht (vergelijk Groenhuijsen en Wiemans, 1989). In navolging van de Commissie Computercriminaliteit heeft de wetgever de

19 Stb. 2009, 245, zie noot 14.

dogmatische keuze gemaakt dat computergegevens geen 'goed' zijn, omdat ze meervoudig zijn (meerdere personen kunnen tegelijkertijd beschikkingsmacht hebben) en het product van geestelijke in plaats van fysieke arbeid; dit is vervolgens bevestigd in de rechtspraak.[20] Met de opkomst van 'virtuele werelden' als *Second Life* en online-computerspellen als *World of Warcraft* is de discussie over 'gegevens als goed' weer heropend, aangezien virtuele objecten in deze werelden *niet* meervoudig zijn en ook vaak geld waard zijn. In lagere rechtspraak wordt het ontvreemden van virtuele objecten dan ook soms gekwalificeerd als diefstal (het wegnemen van een goed).[21] Meningen lopen uiteen of dat een goede keuze is (Hoekman en Dirkzwager, 2009; Moszkowicz, 2009). Duidelijk is dat de rechtspraak – of de wetgever – hierover de komende jaren een standpunt zal moeten bepalen. Ook duidelijk is dat deze discussie vooral op nationaal niveau plaatsvindt; weliswaar wordt de discussie over 'virtuele misdaad' ook internationaal gevoerd, maar Europese regelgeving op dit vlak ontbreekt en valt ook niet snel te verwachten. Dit is een terrein dat zo nauw verweven is met de dogmatiek van het strafrechtssysteem, dat nationale wetgevers hierin eigen keuzes moeten kunnen maken.

Ook om een andere reden is er op onderdelen geen Europese invloed op nationale wetgeving. Over verschillende onderwerpen bestaan grote meningsverschillen, bijvoorbeeld over de toelaatbaarheid van sommige opsporingsbevoegdheden. Voor opsporing van cybercrime is een netwerkzoeking bijzonder relevant: bestanden kunnen via internet op allerlei plaatsen worden opgeslagen en elektronisch bewijs is vluchtig. Daarom moet de politie snel in alle relevante plaatsen kunnen zoeken. Bij de onderhandelingen over het CCV is wel geregeld dat autoriteiten een reguliere doorzoeking moeten kunnen uitbreiden met een netwerkzoeking van rechtmatig toegankelijke computers, maar alleen voor zover deze op nationaal grondgebied staan. Over grensoverschrijdende netwerkzoekingen kon men geen overeenstemming bereiken. De Nederlandse netwerkzoeking blijft dan ook beperkt tot de landsgrenzen en moet daarom voor het verkrijgen van in buitenland opgeslagen bestanden rechtshulp zoeken. België heeft hierin een andere keuze gemaakt

20 HR 3 december 1996, NJ 1997, 574 m.nt. 'tH.

21 Hof Leeuwarden 10 november 2009, LJN BK27764 en BK2773; Rb. Amsterdam 2 april 2009, LJN BH9789, BH9790 en BH9791.

en staat grensoverschrijdende doorzoekingen toe met notificatie achteraf aan de landen waarin computers doorzocht zijn (De Hert en Van Leeuw, 2010, p. 41). Evenmin is op Europees niveau geregeld of de politie op afstand mag 'inbreken' op computers, wat vooral relevant is om een programmaatje (een 'Trojaans politiepaard') te plaatsen dat bijvoorbeeld wachtwoorden of communicatie kan onderscheppen. In Nederland is dit niet toegestaan (Koops en Buruma, 2007; Oerlemans, 2011), hoewel het in de praktijk wel lijkt te gebeuren.[22] Dit is dan ook een onderwerp dat dringend een duidelijke uitspraak van de wetgever behoeft, en dat zal Nederland kunnen en moeten doen zonder invloed van Europa.

Invloed van Nederland op Europa

Tot slot is ook belangrijk om te kijken naar de omgekeerde invloed, van Nederland op Europa. Waar de materiële wetgeving uit 1993 mede een uitwerking was van de destijds bestaande internationale richtlijnen, was de procedurele wetgeving in de Wet computercriminaliteit van Nederlandse bodem. Anders dan bij strafbaarstellingen liep Nederland internationaal voorop in het nadenken over en regelen van opsporingsbevoegdheden in de digitale wereld. De Nederlandse wetgeving heeft dan ook als inspiratiebron gediend voor Aanbeveling 95(13) van de Raad van Europa en vervolgens ook voor het CCV; die invloed kan ook mede te danken zijn geweest aan de voorzitter van de commissie die het CCV ontwierp, Rik Kaspersen, die de totstandkoming van de Wet computercriminaliteit van zeer dichtbij had gevolgd. Bijvoorbeeld de regeling van de netwerkzoeking (beperkt tot de landsgrenzen) in het CCV is vrijwel hetzelfde als de eerdere Nederlandse regeling in artikel 125j Sv. Ook de aandacht in het CCV voor het bevel om computerbeveiliging of gegevensversleuteling ongedaan te maken zal mede geïnspireerd zijn door de Nederlandse regeling uit 1993 van artikel 125k Sv.

22 Kamervragen over het gebruik van spysoftware, 13 oktober 2011, 2011Z20260.

Conclusie

Uit de hiervoor besproken voorbeelden blijkt dat de dynamiek tussen Europese en Nederlandse cybercrimewetgeving verschillende verschijningsvormen heeft. Op hoofdlijnen bestaat de dynamiek vooral uit een Europees regelgevend kader dat op de belangrijkste punten richting geeft aan de nationale wetgeving, waarbij echter wel behoorlijk wat ruimte blijkt te bestaan voor de Nederlandse wetgeving om de Europese regels in te kleuren of op een eigen manier in te passen in het nationale systeem. Aangezien het Europese kader niet allesomvattend is en het Europese wetgevingsproces ook niet heel snel kan inspelen op nieuwe ontwikkelingen, bestaat er daarnaast veel ruimte voor de Nederlandse wetgever om de wet aan te passen op terreinen waar Europa (nog) niets mee doet. Ook op fundamenteel dogmatisch vlak, zoals bij de interpretatie van kernbegrippen als 'goed', kan het Nederlandse recht een eigen lijn volgen. Samenvattend komt dit erop neer dat Europa een basiskader stelt van minimumeisen waaraan het nationale materiële en procedurele strafrecht moet voldoen, die vooral functioneel van aard zijn: bepaalde gedragingen met computers moeten strafbaar zijn en de politie moet bepaalde handelingen kunnen verrichten ter opsporing in een digitale omgeving, maar hoe dit precies wordt ingepast in het rechtssysteem wordt aan de nationale wetgever overgelaten. Daarbij zien we dat de invloed van Europa op het nationale recht groter is in het materiële strafrecht dan in het procedurele strafrecht, deels omdat Nederland dit laatste terrein al behoorlijk had geregeld voordat Europa een kader stelde, maar deels wellicht ook omdat de meningen welke opsporingsbevoegdheden nodig zijn internationaal meer uiteenlopen dan de meningen over wat strafbaar moet zijn. Hoewel het Europese kader de nodige ruimte laat om cybercrimewetgeving in het Nederlandse systeem in te passen, hebben Europese regels ook geleid tot systematische veranderingen in het nationale strafrecht. Soms loopt zo'n verandering parallel aan een bredere tendens in de rechtsontwikkeling, zoals de veranderde ratio van de strafbaarstelling van kinderpornografie past in een toenemende aandacht voor bestrijding van kindermisbruik in de afgelopen decennia; in die gevallen lijkt een systeemverandering dan ook gerechtvaardigd. In andere gevallen zijn de systematische aanpassingen echter meer het resultaat van een eigen interpretatie van de nationale wetgever die niet per se afgedwongen wordt door het

Europese kader, zoals de hoge straf op misbruik van hulpmiddelen; in die gevallen lijkt een systeemverandering meer aanvechtbaar. Dat geldt temeer wanneer een ingrijpende verandering in het systeem nauwelijks op fundamenteel niveau wordt bediscussieerd in Nederland, zoals het aftappen van private netwerken, wellicht omdat men veronderstelt dat het slechts om 'omzetting' van Europese regels gaat. Een wat kritischer houding van het parlement tegenover wetsvoorstellen die belangrijke wijzigingen van het nationale strafrecht behelzen, lijkt mij wenselijk, juist omdat het Europese kader aanzienlijke speelruimte laat om regels in te passen in het nationale systeem.
Een zelfstandige rol van de nationale wetgever zien we ook bij veel onderwerpen die (nog) niet op Europees niveau zijn geregeld. De gedegen discussie over opsporingsbevoegdheden in een digitale omgeving van rond 1990 is een mooi voorbeeld hoe Nederland ook invloed kan uitoefenen op de internationale regelgeving. Wellicht kunnen lopende discussies, zoals over 'diefstal' van virtuele 'goederen', het plaatsen van Trojaanse paarden als opsporingsmethoden of het ontmantelen van botnets,[23] worden aangegrepen voor even gedegen discussies, die vervolgens dan weer kunnen bijdragen aan de Europese discussie – binnen de Raad van Europa of de Europese Unie – over aanpassing van de bestaande cybercrimeregelgeving.

Afsluiting

Is de manier waarop cybercrimewetgeving tot stand komt geschikt voor het reguleren van een dynamisch object als internet? Hoewel het vanwege het grensoverschrijdende karakter voor de hand ligt om internetgerelateerde fenomenen op internationaal niveau te willen regelen, is dat niet altijd mogelijk of wenselijk, zeker bij strafrechtelijke onderwerpen waar de normering sterk samenhangt met culturele en rechtstradities (Prins, 2006).
De dynamiek van cybercrimewetgeving laat zien dat een werkbare combinatie mogelijk is van internationale kaders en nationale invulling en aanvulling. De Nederlandse wet kent een breed vangnet om computercriminaliteit te bestrijden. Vrijwel alle verschijningsvormen van computercriminaliteit kunnen onder

23 Zie noten 22 en 24 en bijbehorende tekst.

strafbepalingen worden gebracht, mede door de ruime formulering van basisdelicten als computervredebreuk (art. 138ab Sr) en gegevensaantasting (art. 350a Sr). Ook de opsporing kan qua bevoegdheden goed uit de voeten met de wetgeving; de praktijk vraagt wel vaak om nieuwe bevoegdheden, zoals het via internet kunnen plaatsen van afluisterprogrammaatjes, maar dat is inherent aan de opsporingstaak, die altijd grenzen van bevoegdheden opzoekt (Enschedé, 1988, p. 223-224).

Hoewel een algemeen probleem van internetregulering is dat techniek zich snel ontwikkelt terwijl wetgeving tijd nodig heeft, kunnen we ook constateren dat cybercrimewetgeving grosso modo goed bij de tijd is en voldoende snel kan reageren op ontwikkelingen in de misdaad. Een probleem is wel dat internationale regulering meer tijd vergt dan nationale wetgeving en dat hierdoor soms de Nederlandse cybercrimewetgeving behoorlijk is vertraagd – zie het wetsvoorstel CCII uit 1999, dat pas in 2006 werd aangenomen. Maar de wetgevingspraktijk laat ook zien dat gaten in de wetgeving op zich snel kunnen worden gedicht door opname van cybercrimebepalingen in reparatie- of omnibuswetten. Op deze wijze is bijvoorbeeld de oplichtingsbepaling aangepast om phishing strafbaar te stellen. Dat wil niet zeggen dat er geen gaten in de cybercrimewetgeving meer zijn of nog kunnen ontstaan, maar wel dat het niet aan de dynamiek van het wetgevingsproces tussen Europa en Nederland hoeft te liggen om die lacunes aan te pakken.

Toch zijn er twee kanttekeningen te plaatsen bij de (inter)nationale totstandkoming van cybercrimewetgeving. Ten eerste is het beleid erg gericht op het klassieke straf(proces)recht: welke handelingen moeten strafbaar zijn, welke opsporingsbevoegdheden zijn nodig? In een internationale context wordt vooral gezocht naar harmonisatie op minimumniveau van het materiële en formele strafrecht en naar het mogelijk maken van wederzijdse rechtshulp (Sieber, 2010, p. 87). Dat geeft een goede uitgangspositie om grensoverschrijdende cybercriminaliteit op te sporen en te vervolgen, zoals de succesvolle aanpak van het Bredolab laat zien; hierbij werd de hoofdverdachte van een botnet, dat vanuit servers in Nederland vele tienduizenden 'zombiecomputers' aanstuurde, op verzoek van Nederland in Armenië gearresteerd en berecht.[24] Maar dit voorbeeld laat ook de

24 De Nationale Cyber Security Strategie (NCSS), bijlage bij Kamerstuk 26 643, nr. 174, p. 2.

beperking zien van het klassieke strafrecht: nadat de verdachte was gearresteerd, wilde justitie het botnet ontmantelen om toekomstig gebruik tegen te gaan, maar daarvoor bestaat internationaal noch nationaal een geschikte juridische grondslag (Koning, 2011). Ook vergt het opsporen van grensoverschrijdende cybercriminaliteit veel capaciteit en kennis van opsporingsdiensten; het belangrijkste knelpunt bij de bestrijding van cybercrime is dan ook niet zozeer de wetgeving, als wel de benodigde investeringen en prioritering in opsporing die nodig zijn om de wet effectief te kunnen handhaven. En hoewel er in het afgelopen decennium grote vooruitgang is geboekt om de capaciteit en kunde van 'cybercops' te faciliteren, valt er nog het nodige te doen op dit vlak.

De tweede kanttekening is dat cybercrime zich transformeert tot een vorm van georganiseerde misdaad, waarin flexibele netwerken met uiteenlopende expertises een grootschalige zwarte markt van cybercrimeprogrammatuur, botnets en financiële gegevens in stand houden (Wall, 2007). Het is de vraag of op langere termijn een strategie van geharmoniseerde minimumwetgeving en wederzijdse rechtshulp, waarin nog steeds veel ruimte is voor nationale invulling en eigen beleidsvorming, opgewassen is tegen georganiseerde cybercrime. Mijn verwachting is dat uiteindelijk meer internationale inspanning nodig zal zijn, waarbij lidstaten een deel van hun nationale soevereiniteit zullen moeten opgeven om internationale en nationale grensoverschrijdende acties (zoals een grensoverschrijdende netwerkzoeking en het ontmantelen van botnets) toe te staan, wil men cybercrime effectief tegenwicht kunnen blijven bieden. In de dynamiek van Europese kaderstelling met veel ruimte voor nationale invulling en aanvulling van cybercrimewetgeving, die tot nu toe goed heeft gewerkt, past ook een dynamische houding om de Europese kaders meer gewicht en sturing te geven wanneer ontwikkelingen in cybercrime daartoe noodzaken.

Literatuur

De Hert, P., F. Van Leeuw
Cybercrime legislation in Belgium
Brussel, VUB/Office of the Federal Prosecutor of Belgium, 2010

Enschedé, C.J.
De burger en het recht. Over macht, gezag en democratie
Amsterdam, Meulenhoff, 1988

Groenhuijsen, M.S., F.P.E. Wiemans
Van elektriciteit naar computercriminaliteit
Arnhem, Gouda Quint, 1989

Hoekman, J., C. Dirkzwager
Virtuele diefstal: hoe gegevens toch weer goederen werden
Computerrecht, nr.4, 2009, p. 158-161

Kaspersen, H.W.K.
Strafbaarstelling van computermisbruik
Antwerpen, Kluwer Rechtswetenschappen, 1990

Koning, M.E.
Terug-hacken als opsporingsmethode
Amsterdam, Universiteit van Amsterdam, 2011 (www.bredolab.nl/wp-content/uploads/2011/11/Terughacken-als-opsporingsmethode-scriptie-Merel-Koning-september-2011-nn.pdf)

Koops, B.J. (red.)
Strafrecht en ICT
Den Haag, Sdu Uitgevers, 2007

Koops, B.J.
The internet and its opportunities for cybercrime
In: M. Herzog-Evans (red.), *Transnational criminology manual*, Nijmegen, Wolf Legal Publishers, 2010a, p. 735-754

Koops, B.J.
Cybercrime legislation in the Netherlands
In: J.H.M. Van Erp en L.P.W. Van Vliet (red.), *Netherlands reports to the eighteenth International Congress of Comparative* Law, Antwerp, Intersentia, 2010b, p. 595-633

Koops, B.J.
Tijd voor Computercriminaliteit III
Nederlands Juristenblad, jrg. 85, nr.38, 2010c, p. 2461-2466

Koops, B.J., Y. Buruma
Formeel strafrecht en ICT
In: B.J. Koops (red.), *Strafrecht en ICT*, Den Haag, Sdu Uitgevers, 2007, p. 77-121

Meulen, N.S. van der
Financial identity theft – Context, challenges and countermeasures
Den Haag, T.M.C. Asser Press, 2011

Moszkowicz, Y.
Een kritische noot bij de 'RuneScape'- en 'Habbohotel'-uitspraken: een illusie is geen goed
Strafblad, jrg. 7, nr. 5, 2009, p. 495-503

OECD
Computer-related crime: Analysis of legal policy
Parijs, 1986

Oerlemans, J.J.
Hacken als opsporingsbevoegdheid
Delikt en Delinkwent, jrg. 41, nr. 8, 2011, p. 888-908

Prins, C.
Should ICT regulation be undertaken at an international level?
In: B.J. Koops, M. Lips e.a. (red.), *Starting Points for ICT Regulation; Deconstructing Prevalent Policy One*-Liners, Den Haag, T.M.C. Asser Press, 2006, p. 151-201

Sieber, U.
General report on internet crimes for the 18th International Congress of the International Academy of Comparative Law, Washington D.C. 2010
Max Planck Institute for Foreign and International Criminal Law, 2010

Vries, U.R.M.T. de, H. Tigchelaar e.a.
Identiteitsfraude: een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen
Utrecht, WODC, 2007 (www.wodc.nl/images/1496_%20volledige_tekst_tcm44-86343.pdf)

Wall, D.
Cybercrime. The transformation of crime in the information age
Cambridge, Polity, 2007

Wiemans, F.P.E.
Computercriminaliteit. Commentaren op het wetsvoorstel computercriminaliteit
Maastricht, Cipher Management, 1991